

**REMARKS**

The Applicants have reviewed the Official Action, mailed November 13, 2002, and have prepared this Amendment in response thereto. Claims 1 and 6 were amended to include the limitations of cancelled claims 12 and 14. Claims 1 – 11, 13 and 15 - 20 remain in the application. The Applicant incorporates by reference the Declarations Under 37 CFR §1.132 of Dr. Mongi Abidi, Dr. Hideki Noda, and Dr. Kyoki Imamura, which were submitted along with the Applicants' Amendment of September 16, 2002, but not acknowledged in the Official Action.

The following remarks will follow the sequence set forth in the Official Action.

**Claim Rejections – 35 USC §103**

Claims 1 - 20 were rejected under 35 U.S.C. §103 as obvious in view of Rhoads in combination with Lofberg. In making this rejection, it was asserted that

“Rhoads discloses a steganography method employing embedded calibration data comprising an information card that stores information data including image data (see figure 24, col. 57, line 30+), wherein the information data includes inherent data that is embedded to the information according to steganography (see col. 2, line 11+); the image is printed on the card (see col. 58, line 58), wherein the image is read using a CCD scanner, and a PIN is used to legitimate the user of the card (see col. 60, line 10+).” *Office Action, Page 2.*

It is likewise asserted that Rhoads discloses that a plurality of code keys are contained in the card and suggests that diskette could be used for the storage medium, but fails to explicitly disclose a memory for storing user information. However, Lofberg is asserted to disclose a data carrier comprising a memory for storing user identification and, in view of Lofberg's teachings, it was asserted that “it would have been obvious for a person of ordinary skill in the art at the time the invention was made to employ the well known smart card into the system of Rhoads in lieu of the basic storage medium for storing user's information”, as “(s)uch a modification would provide

additional storage space to store more information to effectively identify each user". In addition, it was asserted that the memory of Lofberg "could be used as an alternate means for storing information to identify the users and would provide greater processing capability to enable local processing of users' transactions, which would (make) the system more effective and more practical".

The Applicants respectfully disagree with the assertions and, in support, point to the remarks set forth in their Amendment dated September 16, 2002, which are incorporated herein by reference in their entirety. However, in the interest of expeditiously obtaining patent protection for a commercially important group of embodiments of the invention, the Applicants have amended independent claims 1 and 6 to each include the limitations that the card comprise "a visible photograph of the card owner displayed on the card" and that one of the information data and the inherent data stored in memory "comprises a reproduction of the visible photograph of the card owner displayed upon the card". These limitations were included in cancelled claims 12 and 14, which were rewritten in independent form as claims 1 and 6 respectively. For the following reasons, the Applicants assert that independent claims 1, 5 and 6, and dependent claims 2 – 4, 7 – 11, 13, and 15 – 20 that depend therefrom, are unobvious in light of the cited art.

1. All elements of claims 1, 5 and 6 are not found in the cited art

The PLASTIC CREDIT AND DEBIT CARD SYSTEM disclosed by Rhoads (See col. 57, line 30+) has the following features.

- a. An image is printed on the card surface with some optional position fiducials for simplifying the scanning tolerances of the image scanner (Fig. 24).
- b. Some personal identification data such as bar code is marked on the card surface

(Fig. 24).

- c. The visible image data is steganographically embedded with an “orthogonal pattern” or “master snowy image”, essentially “noise”, which does not contain any data to verify the card user, but rather contains a plurality of “transaction tokens” unique to the particular card (Fig. 24 and col. 59, line 22+).
- d. The central network chooses a specific location where it expects to find a “transaction token”, consisting of a specific pattern found in the original image, and verifies that the chosen “token” is identical to that stored in the network. In this manner, the network is said to need only small fraction of the total information embedded in the image to verify the validity of the card (col. 58, line 29+)
- e. The PIN is not stored on the card, nor it is used at the point of sale terminal. It is only appended to information sent to the central accounting network as the only method of verifying the card user. (col. 60, line 24+).

● *No storage of inherent data in memory using steganography*

No memory devices are equipped with the card disclosed by Rhodes. In fact, the statement that “(t)here are no magnetic strips involved,” (col. 58, line 19) clearly teaches that the lack of a memory device is desirable, as a magnetic stripe is a recognized type of memory device. Accordingly, there is no embedding of any information into memory, and certainly no steganographic embedding of inherent data, as claimed by the Applicants in independent claims 1, 5 & 6. Further, Rhodes fails to disclose the claimed reproduction of the photograph, whether stored in memory or otherwise, as claimed by the Applicants in independent claims 1 and 6.

Regarding the assertion that a diskette could be used for the storage medium and that “a

memory circuit is inherently included in the diskette or for storing the code keys”, the Applicants note that, because their claims indicate that it is the card itself that includes the memory device, the use of a separate diskette does not read on the claimed invention and, in fact, would hinder the purpose thereof. Further, Rhoads’ sole teachings regarding a diskette are that “the encoded signal can be distributed in well known ways, including converted to printed image form, stored on magnetic media (floppy diskette, analog or DAT tape, etc.), CD-ROM, etc” (col. 18, line 66+) and “data encoded according to these principles can be stored in various media, including electronic storage media, disks, diskettes” (col.47, line 36+). Thus, Rhoads teaches that such media devices are available for *off-line* distribution of the “information embedded data” and not to serve as a memory device on the card.

Lofberg discloses a data carrier comprising a memory means, designated as reference number “6” in Fig.1, which stores “previously and correspondingly obtained reference bit sequence of finger print data of the card holder.” (col.3, line 57+), and some control information necessary to allow a microprocessor to process finger print data (col.5, line 10+). According to Lofberg:

“At the time when a data carrier according to the invention is issued, the fingertip pattern of one thumb or of a different finger of the owner is recorded. From the recorded information a reference bit sequence, which is unique for the owner or holder, is calculated and this sequence is stored in memory 6 (FIG. 1). When the holder later on is to identify himself against his data carrier, the fingertip information should again be recorded in order to allow for a comparison against the reference bit sequence. This means substantially two problems. First, it must be safeguarded that the direction of the fingertip relative to the sensing surface will be the same as during the recording of the reference bit sequence or otherwise it must be possible to modify the recorded information with respect to a different orientation of the fingertip. Second, the information which is recorded in the sensing device must be read and processed in a way which is reproducible.”  
*Lofberg, Col. 8, Lines 48 – 55.*

Lofberg goes into great detail in its discussion of the specifics of reading and comparing fingerprint patterns, and places emphasis on the fact that the direct comparison of fingerprints at the

identification point eliminates any need for a PIN or verification by a central network. However, because of the supposed "fail safe" identification provided by fingerprint comparison, Lofberg makes no effort to hide the information stored in the memory, and certainly does not embed any information within the memory using steganography, as claimed by the Applicants in each of claims 1, 5 and 6. Further, Lofberg provides no reference to a photograph either on the carrier or stored into memory, as claimed by the Applicants in claims 1 and 6.

- *No output of any read information data*

In addition to the fact that none of the references disclose a memory containing steganographically embedded inherent data, as claimed in claims 1, 5 and 6, the Applicants reiterate their assertion that the card system of Rhoads does not include any "output means for outputting the read information data", as claimed in claims 5 and 6. Further, such an output means is not found in Lofberg, or any of the other cited references. Lofberg provides an output signal that indicates the favorable or unfavorable result of the fingerprint authentication process, but does not output any of the data stored in the memory; i.e the reference signals corresponding to the fingerprints stored in the memory. Such an output signal is likewise not found in any of the other cited references.

2. There is no motivation or suggestion to combine or modify the cited references

The Applicants further assert that there is no motivation or suggestion to combine or modify Rhoads to include claimed memory, the claimed reproduction of the owner's photograph, the claimed embedding of inherent data into memory according to steganographic information hiding, or the claimed output of read information data.

- *Rhoads explicitly teaches away from the methods of Lofberg*

As noted above, Rhoads eschews the use of magnetic strip or other memory device. Further,

in asserting the inadequacy of memory devices, such as magnetic strips, Rhoads expressly teaches away from the use of the same fingerprint identification techniques taught by Lofberg, by stating:

“Applicant is aware of a similar idea employed in the very high precision recording of credit card magnetic strips, as reported in the Feb. 8, 1994, Wall Street Journal, page B1, wherein very fine magnetic fluxuations tend to be unique from one card to the next, so that credit card authentication can be achieved through pre-recording these fluxuations later to be compared to the recordings of the purportedly same credit card.

Both of the foregoing techniques appear to rest on the same identification principles on which the mature science of fingerprint analysis rests: the innate uniqueness of some localized physical property. These methods then rely upon a single judgement and/or measurement of "similarity" or "correlation" between a suspect and a pre-recording master. Though fingerprint analysis has brought this to a high art, these methods are nevertheless open to a claim that preparations of the samples, and the "filtering" and "scanner specifications" of Melen's patent, unavoidably tend to bias the resulting judgement of similarity, and would create a need for more esoteric "expert testimony" to explain the confidence of a found match or mis-match. An object of the present invention is to avoid this reliance on expert testimony and to place the confidence in a match into simple "coin flip" vernacular, i.e., what are the odds you can call the correct coin flip 16 times in a row.” *Rhoads, Col. 2, line 47 – Col. 3, line 4.*

Because Rhoads specifically seeks to avoid the “esoteric “expert testimony”” required by fingerprint identification systems, and as Lofberg was cited by Rhoads during the prosecution of its patent, it can reasonably be presumed that the above passage was specifically directed to the system of the Lofberg patent. Accordingly, as Rhoads expressly teaches away from fingerprint verification systems, and as Lofberg was cited as one of such systems by Rhoads, it is asserted that there would be no motivation to combine the Rhoads and Lofberg references to obtain the Applicants’ claimed invention.

- *No motivation to add memory to store a reproduction of the owner’s photograph or password*

In addition to the express teaching of Rhoads away from Lofberg, as asserted by the

Applicants in the Amendment of September 16, 2002, the methods disclosed in the Rhoads reference are primarily directed to the authentication of the identity of a signal, computer file, image, card, or the like, rather than the authentication that the holder of such a signal, computer file, image or card is the rightful owner. Accordingly, there is no motivation provided within Rhoads to modify the card to include a memory, or “a reproduction of the visible photograph of the card owner” in order to authenticate that the holder of such a signal, computer file, image or card is the rightful owner.

The Applicants’ assertion was supported by the Declarations Under 37 CFR §1.132 of Dr. Mongi Abidi, Dr. Hideki Noda, and Dr. Kyoki Imamura, each of whom declared the “methods disclosed in the Rhoads reference are primarily directed to the authentication of the identity of a signal, computer file, image, card, or the like”, and “based upon the teachings of Rhoads, I would have no motivation to modify the Rhoads methods to authenticate that the holder of such a signal, computer file, image or card is the rightful owner.”

Lofberg likewise fails to provide such motivation. As noted above, Rhoads is directed solely to the authentication of the card and not to the authentication of the user. Conversely, Lofberg represents a completely different approach, in which no effort is made to insure that the card itself is authentic. Rather, Lofberg is concerned solely with the determination of whether the fingerprint data stored in the memory of the card matches the fingerprint data obtained by a live scan of a person seeking to use the card. If this data is a match, the verification device indicates this fact and the transaction is presumably allowed to continue. It is important to note that there is no discretion on the part of the security person, clerk, or any other person who is requesting authentication, in making this determination. Accordingly, no information is stored in memory to allow such a person to make a contrary determination.

The reason for Lofberg's avoidance of in-person analysis of data and determination of authenticity is readily apparent by looking to the "Background of the Invention". Lofberg states that:

"A general problem when data cards are used is the fact that a lost or stolen data card may be used without authorization by a different person. This problem may be eliminated if the user is obliged to verify his right before the data card may be used.

In the case of data cards intended for manual handling, the verification may be carried out in that the user verifies his identity by presenting a different identification document. Normally, however, a certification is not required when such a data card is used, among other things due to the fact that this will create a delay and give rise to a long line of people at the places of use. Instead the active control or check is carried out by means of so-called black lists comprising the numbers of all blocked accounts, which may have been blocked due to the fact the account holder has not fulfilled his obligations towards the accounting organization or the fact that the account holder has reported the card as lost. The black lists, being up-dated regularly, mean a significant increase of work at the places of use. Moreover, it is possible that a blocked account will not be observed during a manual check. As a consequence, the card will be used despite the fact that it should not. Furthermore a card, which has been lost for example, may be misused from the time it is reported as lost until an updated black list is available." *Lofberg; Col. 1, line 46 – Col. 2, line 3.*

As these paragraphs make clear, the unauthorized use of a lost or stolen card is the problem to be solved, and it is conceded that it is impractical to conduct a in-person verification using an "identification document"; presumably a drivers license, passport, etc., due to the fact that such verification causes delays and gives rise to "a long line of people at the places of use." Given this focus on avoiding the delays caused by in-person verification, the Applicants assert that Lofberg teaches away from the inclusion of any information that could be used during an in-person analysis to make a determination of authenticity. Thus, Lofberg likewise teaches away from the storage of the claimed reproduction of the owner's photograph, as the only purpose of such a photograph would be to enable the same in-person analysis that it seeks to avoid. Finally, as Lofberg teaches that it is desirable



to avoid in-person screening, there would certainly be no need for the claimed output of read information data, which is again provided solely for this purpose.

It is likewise noted that Lofberg teaches away from the storage of a personal identification number (PIN), or other type of “password” or “customized key”, into memory, as claimed in claims 5 and 6. In fact, Lofberg devotes an entire column of his “Background of the Invention” to the drawbacks of PIN, or other password based systems. *See Lofberg, Col. 2, line 16 to Col. 3, line 14.* Accordingly, the Applicants likewise assert that there would be no motivation to modify the card of Lofberg to include the password claimed in claim 5, or the customized key of claim 6.

For the reasons set forth above, the Applicant asserts that there would be no motivation to combine Rhoads and Lofberg to obtain a system having the applicant’s claimed memory, the reproduction of the owner’s photograph of claims 1 and 6, the password of claim 5, or the customized key of claim 6.

- *No motivation to embed data into memory according to steganographic information hiding or to include the claimed output of read information data*

The Applicants further assert that Rhoads use of steganography is vastly different from that of the Applicants and, therefore, even if there were motivation to include a memory that there would be no motivation to embed information onto the memory using steganography, or to provide an output of this information data once it is read from the card.

As noted above, the use of steganography in Rhodes is intended to embed a plurality of “transaction tokens” within an image that can later be identified by a card scanner and compared with the version of scanned image stored in a remote location. Thus, Rhoads avoids the use of a memory by hiding the means for authenticating the card within the image and then using a secure network to

verify that the hidden means are there. In this way, Rhoads is similar to Lofberg, as each check for specific information on the card and provide an automatic authentication based solely upon this automated check. Further, neither Rhoads nor Lofberg are readily susceptible to the alteration of a valid card. Rhoads avoids this by keeping a “private key” at the network location, which insures that there is one set of data that is incorruptible. Lofberg does this by embedding a reference bit sequence that corresponds to the authorized user’s fingerprint. This sequence is developed using the complex techniques enumerated in the Lofberg patent and, therefore, it would be nearly impossible for a would-be forger to alter these bits to reflect his/her own fingerprints. Thus, neither Rhoads nor Lofberg provide any motivation to hide information within the card in order to prevent use of altered cards.

Conversely, the Applicant’s card and system provide no such automatic authentication and, absent the hiding of the inherent data in memory using steganography, would be readily susceptible to alteration. The Applicant relies directly on the in-person verification, which is accomplished by a reading the information data, stored in the memory, including the inherent data, comparing a photograph with that of the user, and/or querying the user about other inherent data read from memory that authenticates a legitimacy of a card owner. Thus, if the read data matches the other data available to the person charged with verification, the card will appear to be legitimate. Unfortunately, this creates a risk of alteration that is not present in either Rhoads or Lofberg.

Absent the Applicants’ steganographic embedding, an unauthorized user could replace the photograph on the face of the card, and either the embedded photograph or other data, with his own, and then could freely use the card. These circumstances, which are not found in either Rhoads or Lofberg, are what motivated the Applicants to use steganographic embedding of the data, which is not readily altered or replaced. Thus, it is asserted that neither Rhoads nor Lofberg would be motivated to

use steganographic embedding of data stored in memory.

Finally, the Applicants note that the systems of Rhoads and Lofberg are each specifically designed to avoid a transmission of the actual data and, therefore, there would be no motivation to modify either system to include the Applicants' claimed "output means". With regard to Rhoads, this assertion is supported by the Declarations, in which each Declarant declares that "the card disclosed in the Rhoads reference does not provide any authentication that the user of the card is the owner of the card and does not include any "output means for outputting the read information data", as claimed in the Applicant's claims 5 – 12" and "because the system disclosed in the Rhoads is specifically designed to avoid a transmission of the actual data, I would have no motivation to modify the system to include such an "output means". With regard to Lofberg, the Applicants point to the remarks set forth above with regard to its teaching away from in-person authentication as support for this assertion.

For the reasons set forth above, the Applicants assert that the neither Rhoads nor Lofberg discloses or suggest the claimed storage of inherent data in memory using steganography, or the claimed output of read information from memory. The Applicants further assert that there is no motivation or suggestion to modify Rhoads, or to combine Rhoads and Lofberg, to include claimed memory, the claimed reproduction of the owner's photograph, the claimed embedding of information data into memory according to steganographic information hiding, or the claimed output of read information data.

### Conclusion

It is felt that a full and complete response has been made to the Official Action and, as such, places the application in condition for allowance. Such allowance is hereby respectfully

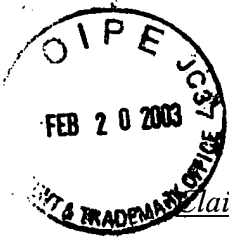
requested. If the Examiner feels, for any reason, that a personal interview will expedite the prosecution of this application, he is invited to phone the Applicants' attorney at his new address, as set forth below.

Respectfully submitted,



Date February 13, 2003

Michael J. Persson  
Attorney for Applicant  
Registration No. 41,248  
Lawson & Persson, P.C.  
67 Water Street, Suite 103  
Laconia, NH 03246  
Phone: 603-528-0023  
Fax: 603-528-3332



claims 1 & 6, with indicia of amendment

1. An information card comprising a visible photograph of a card owner displayed upon the card and a memory that stores information data, the information data comprising one of image data and acoustic data;

wherein the information data contains inherent data that is embedded in the information data according to steganographic information hiding; [and]

wherein the inherent data comprises data that authenticates a legitimacy of a card owner of the information card; and

wherein one of the information data and the inherent data comprises a reproduction of the visible photograph of the card owner displayed upon the card.

6. An information card system comprising:

an information card comprising a visible photograph of a card owner displayed upon the card and a memory that stores information data, wherein the information data comprises one of image data and acoustic data, wherein the information data comprises inherent data that is embedded in the information data according to steganographic information hiding, wherein one of the information data and the inherent data comprises a reproduction of the visible photograph of the card owner displayed upon the card; and,

a data processing terminal comprising input means for submitting a customized key, inherent data extracting means for extracting the inherent data with the use of the

submitted customized key, and output means for outputting the extracted inherent data.

RECEIVED  
FEB 24 2003  
TECHNOLOGY CENTER 2800